



# Nøglehåndtering

Sikkerhed04, Aften



# Basalt problem

- Al kryptografisk sikkerhed er baseret på nøgler som ikke er kryptografisk beskyttet
- I stedet må disse nøgler beskyttes fysisk



# Løsninger

- Passwords
  - noget du *ved*
- Hardware
  - noget du *har*
- Biometri
  - noget du *er*



# Password

- Et password er en sekvens af tegn som kun ejeren og systemet kender, fx
  - QWERTY
  - 8676
  - Kis#1erT\$



# Angreb/aspekter

Aspekt	Angreb
Valg af password	Gætte password
Brug af password	Se password under brug
Ejers opbevaring	Stjæle password fra ejer
Systemets opbevaring	Stjæle fra systemet



# Valg af password

- Nøglerum: lange passwords = mange muligheder
  - 4-cifret PIN-kode: 10.000 muligheder
  - 8 unix-tegn:  $\approx 2^{52}$
- Praktisk begrænsning
  - Maksimalt huske 12 under stress



# Passphrases

- Længde er ikke nok - kvalitet er afgørende
- Passphrases:
  - Kursus i sikkerhed nummer 1 er Top-dollar
  - Kis#1erT\$
- Ligeså godt som tilfældigt valgte strenge!



# At gætte et password

- Forsøg (mere eller mindre intelligent) at logge på 'pagter' indtil det lykkes
- Efter 3 forsøg blokeres kontoen
- 😊 😞 ?!
  - Godt hvis angriberens mål er at logge ind
  - Skidt hvis målet er at forhindre dig (og evt. andre) i at logge ind



# Stjæle password under transmission

- Kikke folk over skulderen
  - Spyware
- Falsk hardware
- Lytte på netværk
  
- Løsninger involverer (sjovt nok)
  - Crypto
  - Hardware
  - Biometri



# At stjæle et password fra brugeren

- Hvis det er skrevet ned?
  - En lap i affaldsspanden
- PIN-kode-husker
- Social Engineering...



# Social engineering

- 336 studenter blev pr. mail bedt om at udlevere deres password for at validere password-databasen
- 138 returnerede deres password!!!!
- Mere (mindre?) sofistikerede metoder:
  - Ringe til firmaet "Benjamin": Jeg er sikkerhedschef hos IBM, jeres software har et problem (måske endda "Benjamin"s skyld), jeg skal bruge dit password...



# Social engineering - modtræk

- En af de bedste måder at bryde ind i systemer
- Information og uddannelse
- Teknik:
  - Hardware
  - Biometri



# At stjæle password fra systemet

- Password-databasen i klartekst
- En udbredt metode er at gemme en kompliceret funktion af passwordet og ikke passwordet selv
- Men, pga. dårligt valgte passwords fejler dette også ofte



# Password-DB vha. envejsfunktioner

- Tabel med indgange:
  - u, user
  - $F(\text{pwu})$
- Hvor  $f$  er en funktion som er let at beregne men svær at inverttere



# Dictionary attack

- Envejs-funktionen er kendt
- Tag en ordbog over sandsynlige passwords, pw
- Beregn  $f(\text{pw})$  indtil der findes match
- Op til 25% succesrate i praksis  
– passphrases



# Passwords - overblik

Aspekt	Angreb	Modtræk



# Hardware

- Øget fysisk beskyttelse mod afsløring af nøgle
- Netop en kopi af nøgle
  - Off-line angreb
  - Besværliggøre kopiering
  - Sikre opdagelse af kopiering



# Chip-kort

- Som fx magnetkort, med
  - CPU, RAM, I/O, sågar RSA co-processor
- Fx det nye DanKort, SIM-kort til mobiltelefoner, ...
- Fysisk indbrud svært!



# Analyse af strømforbrug

- Naiv implementation af RSA-kryptering
  - Scanne bits i nøgle:
    - Hvis 0, så et forløb af instruktioner
    - Hvis 1, så et andet
  - *Meget* stor forskel i strømforbrug ved de to
  - Aflæs strømforbrug => private-key i klartekst!



# Dårligt API

- Forsøg at gætte PIN
- Hvis gæt forkert, laves bestemte operationer som kan lures (vha strømforbrug)
- Send "RESET", og undgå at antal forkerte gæt tælles op



# Tamper resistance

- Amerikansk standard: FIPS
- Skal kunne detektere
  - Nedfrysning
  - Rystelser
  - Eksplosioner
  - Magnetfelter
  - ...

# IBM 4758

- Evalueret til højeste FIPS-level
- Typisk brugt af banker
- Ingen kendte angreb (Der var tidligere et angreb baseret på en fejl i API'et)





# Autenticitet – igen igen

- Scenario:
  - RSA private-key i IBM4758, som kun kan tilgås hvis man har smart-card og kender PIN-koden til dette
- Instruer – vha. downloadet software - systemet om at underskrive et dokument
- Hvad skrives faktisk under?!



# Hardware - overblik

- Beskyttelse
  - Fortrolighed
  - "Bevis" for brud på do.
- Angreb
  - Dårlige API'er
  - Uforudsete sideeffekter
  - Kontrol over både hardware og software?

# Biometri

- Traditionelt:
  - Menneske-menneske
  - Baseret på underskrifter, fotos, etc.
- Her:
  - Menneske-maskine
  - Baseret på biologiske kendetegn



BornholmsTrafikken



# Generel løsning

- Funktion fra individ til data
  - Baseret på særlige biologiske karakteristika
  - Database over disse
- Identifikation:
  - Foretag måling
  - (Gen-)beregning funktion
  - Sammenlign med database



# Falske negative og positive

- Falsk negativ: du afvises selvom du rettelig er i systemet
- Falsk positiv: du godkendes selvom du ikke er i systemet
- Den konkrete anvendelse afgør hvad der er "acceptabelt"



# Teknologier

- Iris-scanning
  - Fingeraftryk
  - Ansigtsform
  - Håndgeometri
  - Tale
  - ...
- 
- Specielt de to førstnævnte er gode



# Fordele og ulemper

- Du har altid dig selv med
- Anonymitet
- Beskyttelse af system
- Fysisk forandring af individet
- Bemærk: Dit fingeraftryk er ikke en signatur!



# Nøglehåndtering - overblik

